15 14
~~20.~~ The computer system of claim ~~19~~, wherein the trusted operating system further causes the processing unit to validate each application requesting access to the downloaded information using the access predicate, and decrypts the seed value for use by a validated application.

16 13
~~21.~~ The computer system of claim ~~18~~, wherein the storage key used to encrypt the downloaded information is specific to an application.

17 13
~~22.~~ The computer system of claim ~~18~~, wherein the storage key used to encrypt the downloaded information is specific to a user.

23. (Canceled)

24. (Canceled)

REMARKS

The above Amendments, in conjunction with the following remarks, place the application in immediate condition for allowance. Accordingly, Applicant respectfully requests entry of the Amendments and favorable consideration of the application.

§ 102 Rejections

Claims 1-2, 5, 13-14 and **23-24** are rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Herbert (US # 5,757,919). Claims 1-2, 5, 13-14 and 23-24 have been canceled without prejudice.

Allowable Subject Matter

Claims 18-22 are expressly allowed.

Claims 3-4, 6-12, and **15-17** are objected to as being dependent upon rejected base claims, but are allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Accordingly, claims 3-4 and 6-9 have been amended to include base claim 1. Claims 6 and 7 have been additionally amended to include intervening claim 5. Therefore, claims 3-4 and 6-9 are allowable.

Claims 10-12 depend from claim 9, and are therefore also allowable.

Claims 15-17 have been amended to include base claim 14. Claims 15-17 are therefore allowable.

The Office is now free to remove the objection to claims 3-4, 6-12, and 15-17.

Conclusion

All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

B

Respectfully Submitted,

Dated: 10/22/02

By: Nathan R. Rieth

Nathan R. Rieth
Reg. No. 44302
(509) 324-9256

B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/227,568
Filing Date 1/08/99
Inventorship ..... England
Applicant..... Microsoft Corporation
Group Art Unit 2662
Examiner ..... Jack, Todd M.
Attorney's Docket No. MS1-282USC3
Title: Key-Based Secure Storage

Amended Claims With Markings To Show Changes Made

Claims 3-4, 6-9, and 15-17 have been changed by the accompanying Response To Final Office Action relative to their immediate prior versions. A marked up version of claims 3-4, 6-9, and 15-17 is therefore submitted below in accordance with 37 C.F.R. §1.121(c).

3. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

[The computerized method of claim 1, wherein the storage key is an application storage key and obtaining the application storage key comprises:]

generating a seed value;

producing a hash seed value based on the seed value using a one-way hash function; [and]

generating an [the] application storage key from the hash seed value;

encrypting the information using the application storage key; and

associating the access predicate with the encrypted information.

B

4. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

[The computerized method of claim 1, wherein the storage key is a user storage key and obtaining the user storage key comprises:]

generating a seed value;

producing a first hash seed value based on the seed value using a one-way hash function;

producing a second hash seed value based on the seed value and a user identifier using a keyed hash function; [and]

generating a [the] user storage key from the second hash seed value;

encrypting the information using the user storage key; and

associating the access predicate with the encrypted information.

6. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

obtaining an operating system storage key;

B

encrypting the access predicate with the operating system storage key; and

[The computerized method of claim 5, further comprising:]

encrypting a plurality of other storage keys using the operating system storage key, wherein the other storage keys are selected from the group consisting of application storage keys and user storage keys.

7. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

[The computerized method of claim 5, wherein obtaining the operating system storage key comprises:]

generating a seed value; [and]

generating an [the] operating system storage key based on the seed value; and

encrypting the access predicate with the operating system storage key.

8. (Twice Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

B

[The computerized method of claim 1, wherein the storage key comprises an application storage key and a user storage key to encrypt information containing portion specific to an application and a portion specific to a user, and obtaining the storage key comprises:]

generating a seed value for the application;

producing an application hash seed value based on the seed value for the application using an application-specific one-way hash function;

generating an application storage key from the application hash seed value;

generating a seed value for a [the] user;

producing a first user hash seed value based on the seed value for the user using a one-way hash function;

producing a second user hash seed value based on the first user hash seed value and a user identifier using a keyed hash function; [and]

generating a user storage key from the second user hash seed value, the application storage key and the user storage key to encrypt information containing a portion specific to an application and a portion specific to the user;

encrypting the information using the application storage key and the user storage key; and

associating the access predicate with the encrypted information.

9. (Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

[The computerized method of claim 1, further comprising:]

storing the storage key in a key vault provided by a third-party; and

recovering the storage key from the key vault.

15. (Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit to generate an operating system storage key based on an identity for the operating system and [The computer system of claim 14, wherein the operating system storage key is further] based on a seed.

16. (Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit

B

to generate an operating system storage key based on an identity for the operating system;

[The computer system of claim 14, further comprising:]

an application specific one-way hash function executed from the computer-readable medium by the processing unit, wherein the application specific one-way hash function causes the processing unit to generate an application storage key from a hashed seed; and

a generate application key function executed from the computer-readable medium by the processing unit, wherein the generate application key function causes the processing unit to generate the hashed seed from an application seed.

17. (Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit to generate an operating system storage key based on an identity for the operating system;

[The computer system of claim 14, further comprising:]

a key-hash function executed from the computer-readable medium by the processing unit, wherein the key-hash function causes the processing unit to generate a user storage key from a hashed seed and an identity for the user;

B

a one-way hash function executed from the computer-readable medium by the processing unit, wherein the one-way hash function causes the processing unit to generate the hashed seed from a previously hashed seed; and

a generate user key function executed from the computer-readable medium by the processing unit, wherein the generate user key function causes the processing unit to generate the previously hashed seed from a user seed.

Respectfully Submitted,

Dated: 10/22/02

By: Nathan R Rieth

Nathan R Rieth
Reg. No. 44302
(509) 324-9256; X233

B